Ki a felelős cloud szolgáltatónál tárolt adatainkért? – Cloudban tárolt adataink mentése és archiválása

Dravecz Tibor, INTEGRITY Kft.
Bencze Zoltán, INTEGRITY Kft.
Bakos Dániel, egyetemi hallgató, Óbudai Egyetem

2022. május 23.

Ki felel a felhőben tárolt adatainkért?

Mi (előfizető) vagy a szolgáltatónk? – Vagy megoszlik a felelősség?

A felhő, illetve a felhőszolgáltatás más, mint az on-premise kiszolgálás. Más a biztonság és az adatvédelem, más a felelősség, más a megfelelősség.

- Felelősség tekintetében a fő vezérvonal az ún. **osztott felelősség modell (shared responsibility model)**, azonban más ez a modell az elméletben, és más a gyakorlatban – a gyakorlatban a dolgok bizony trükkösek lehetnek.

Nagyon fontos megismernünk és tisztában lennünk azzal, hogy

- pontosan ki is a felelős az adatainkért - mi vagy a szolgáltatónk (CSP)?
- Mikor és miben vagyunk mi a felelősek, mikor és miben a szolgáltatónk?

- Mennyire ismert, hogy kié a felelősség?
- Mennyire ismert az osztott felelősség modell (shared responsibility model)?
- Mennyire vannak a döntéshozók és az informatikusok tisztában
  - az osztott felelősséggel,
  - illetve azzal hogy, adatvesztés mikor, mi miatt és hogyan történhet a felhőben,
  - készül-e adataikról mentés?

"The shared responsibility model of the cloud is a nice theory and, as with all theories, it is the practical application where things can get tricky." – https://www.isc2.org/Articles/Responsibility-and-Accountability-in-the-Cloud

Microsoft 365 adatok mentése

Szükség van-e arra, hogy mentsük Microsoft 365 szolgáltatásokban tárolt adatainkat?

Tudjuk, hogy az M365 szolgáltatás keretében

- több példányban tárolja a Szolgáltató az adatainkat, méghozzá georendundánssan,
- valamint különféle adatvédelmi megoldásokat alkalmaz (verziózás, Recycle Bin stb.),

mindazonáltal **ismerni kell az M365 szolgáltatás korlátait is**,

- **mind technikai, mind szerződéses korlátok is vannak**.

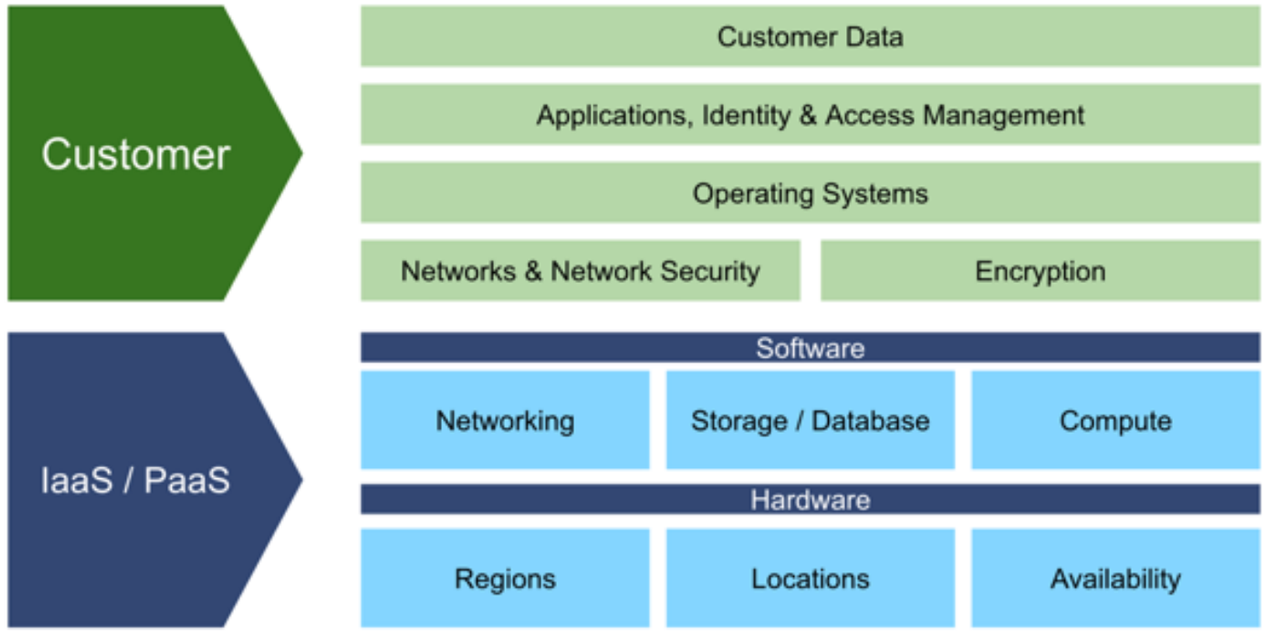
Osztott felelősség modell (shared responsibility model)

Feltétlenül tisztában kell lenni, hogy ki és mennyiben felel adatainkért!

Mi is az az osztott felelősség modell?

A Microsoft 365 és jellemzően hasonló szolgáltatásoknál (Google, AWS stb.) a szolgáltatók az ún. **osztott felelősség (shared responsibility) modell**t alkalmazzák, mely fő vonalakban azt jelenti, hogy

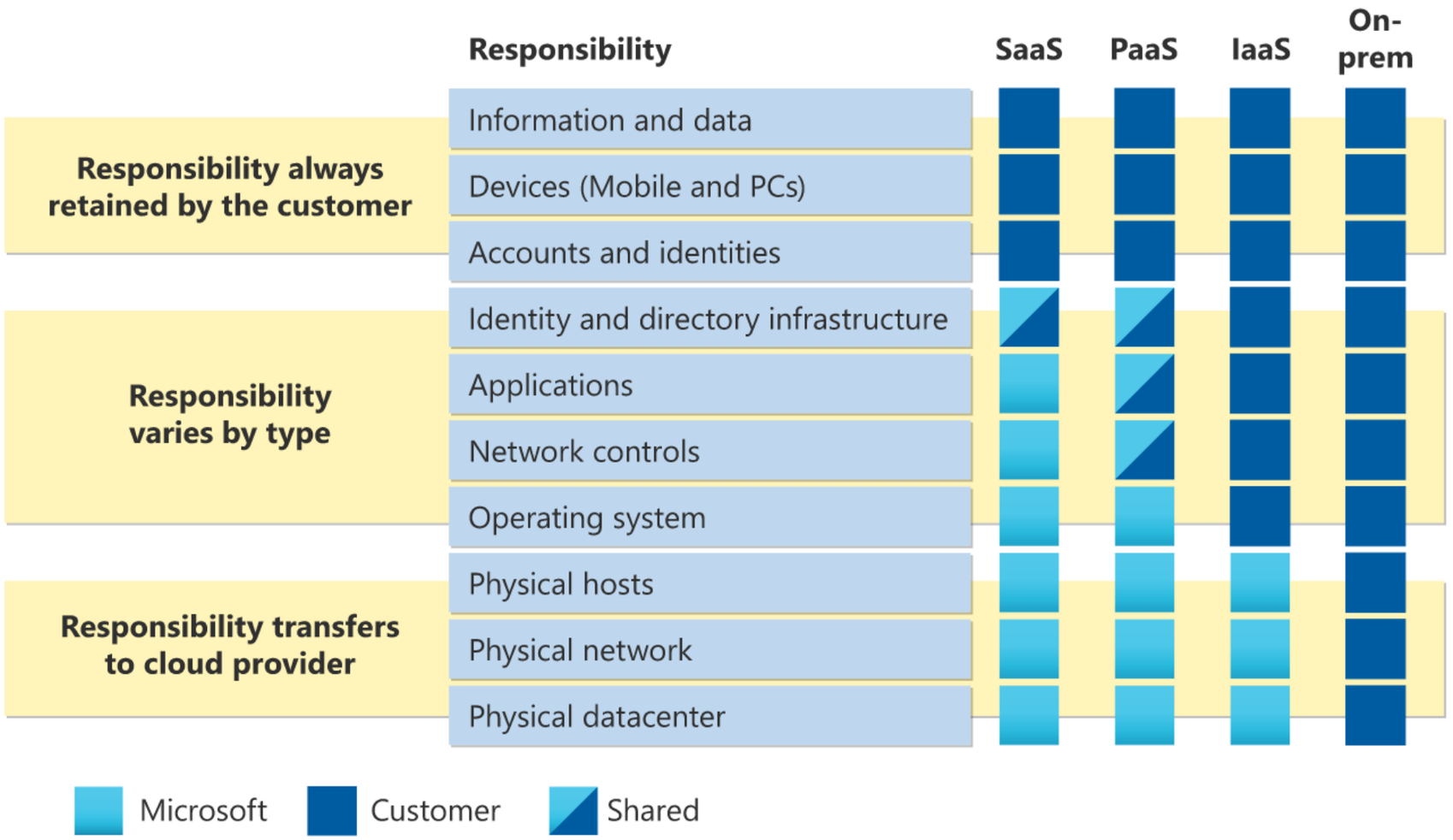
- a Szolgáltató (Microsoft) felel a szolgáltatás működéséért és rendelkezésre-állásáért,
- **az Ügyfél pedig a saját adataiért felel**.



https://devops.com/mastering-the-shared-responsibility-model/

Adatokért és információkért az Előfizető felel.

A Szolgáltató felelősségi köre.



https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

"You are responsible to protect your data from human error (due to malicious activity or innocuous accidents), misconfigured workflows, hackers, and viruses.

- **Backing up your users and data is truly your responsibility and if you are not proactive about that,**
- **any help you get from Microsoft in times of crisis is minimal at best."**

https://www.backupify.com/blog/office-365-backup-7-things-you-need-to-know

Mindenhol történhet hiba

Akármelyik szolgáltató szolgáltatását is vesszük igénybe, a szolgáltatónál történhet hiba – a szolgáltatóval, illetve szolgáltatásaival szemben visszaéléseket követhetnek el, lehet külső és belső visszaélés; visszaélés és hiba a leggondosabb és legszakszerűbb működés mellett is történhet.

Gondoljunk csak a **Log4shell** sérülékenységre mely akár a legfelkészültebb és leggondosabban eljáró szolgáltatónál is egypontbeli olyan hibához vezethetett, mely teljes hozzáférést tesz támadónak lehetővé akár kritikus rendszerhez.

A Microsoft kiváló szolgáltatónak bizonyult védelmi szempontból az M365 (korábban O365) szolgáltatások nyújtása során, de sajnos **hiba még náluk is bekövetkezhet**, akkor is, ha a védelmük egyre jobbá válik.

És persze a Szolgáltató (Microsoft) felelőssége korlátozott is.

Teljesen ne bízzunk meg senkiben, kritikus adatainkat magunk is védjük – válasszunk megbízható szolgáltatót, de saját magunk is védekezzünk!

Adatvesztés speciális okai

A teljesség igénye nélkül:

- Jogosulatlan hozzáférés potenciális következményei
- Véletlen törlések (beleértve felülírások)
- Ügyféloldali rendszeradminisztrációs hibák
- Verziózás
    - nem minden verziózott,
    - verziózás nem a file vagy objektum védelmére szolgál,
    - törölt file minden verziója törlésre kerül,
    - jogosulatlan hozzáféréssel akár minden verzió felülírható.
- Retenciók korlátai
- Retenciós policy rések
- Inaktív felhasználók
- Visszaállítás is okozhat adatvesztést (pl. felülírás történhet)
- Bizonyos törlésre kijelölt adatok (pl. Recycle Bin adatai) nem kereshetők az M365-ben

Összefoglaló: Mit ellen és miért kell az ügyfélnek védekezni?

A Szolgáltató (Microsoft) nem felel az Ügyfél adataiért.

- Az M365 szolgáltatásban, annak hibája miatt is történhet adatvesztés,
- még inkább előfordulhatnak adatvesztések az M365 szolgáltatás hibáin kívül.
- M365 üzemkiesés esetén is el kell érni az Ügyfélnek a legkritikusabb adatait.

Az Ügyfélnek védekeznie kell:

- véletlen törlés,
- külső támadók,
- belső visszaélések,
- gondatlan belső üzemeltetés következményei,
- zsarolóvírus és egyéb malware károk ellen,
    - zsarolóvírus már a felhasználók eszközein titkosíthatja az adatokat,

továbbá

- távozó alkalmazottak adatait is el kell érni,
- az M365-ös retenciós idők nem mindig elégségesek,
- retenciós policy nem kívánt/várt változásaira is fel kell készülni,
- az M365 visszaállítási lehetőségek korlátozottak,
- M365 nem biztosít gyors és teljesen kielégítő visszaállítási lehetőségeket, (Point-in-time recovery /PITR/ lehetőségének a hiánya),

– a teljesség igénye nélkül a főbb dolgokat kívántuk itt kiemelni.

Fontos viszont, hogy tökéletes mentési megoldás nincs, mindig fel kell mérni, meg kell ismerni az általunk alkalmazott, igénybe vett backup és archiválási megoldás korlátait is.

Hogyan és mivel védekezzünk-védekezhetünk?

- Az M365 szolgáltatás gondos és szakszerű igénybe vételével,
- szervezet szinten kialakított, jól tervezett, jól karbantartott és felhasználóinknál kikényszerített policy alkalmazásával,
    - különös tekintettel a retenciós és törlési rendre,
- third-party mentési megoldás (szoftver/szolgáltatás),
    - pl. VEEAM Backup & Recovery for Microsoft Office 365 igénybevételével,
- és megfelelően kialakított mentési renddel és archíválással,
    - off-line és off-site mentéssel és archíválással,
    - megfelelő katasztrófatervvel és felkészültséggel,
    - jó dokumentálással,
    - megfelelő ellenőrzésekkel, tesztekkel, gyakorlatokkal, felülvizsgálatokkal és audittal.

Melléklet

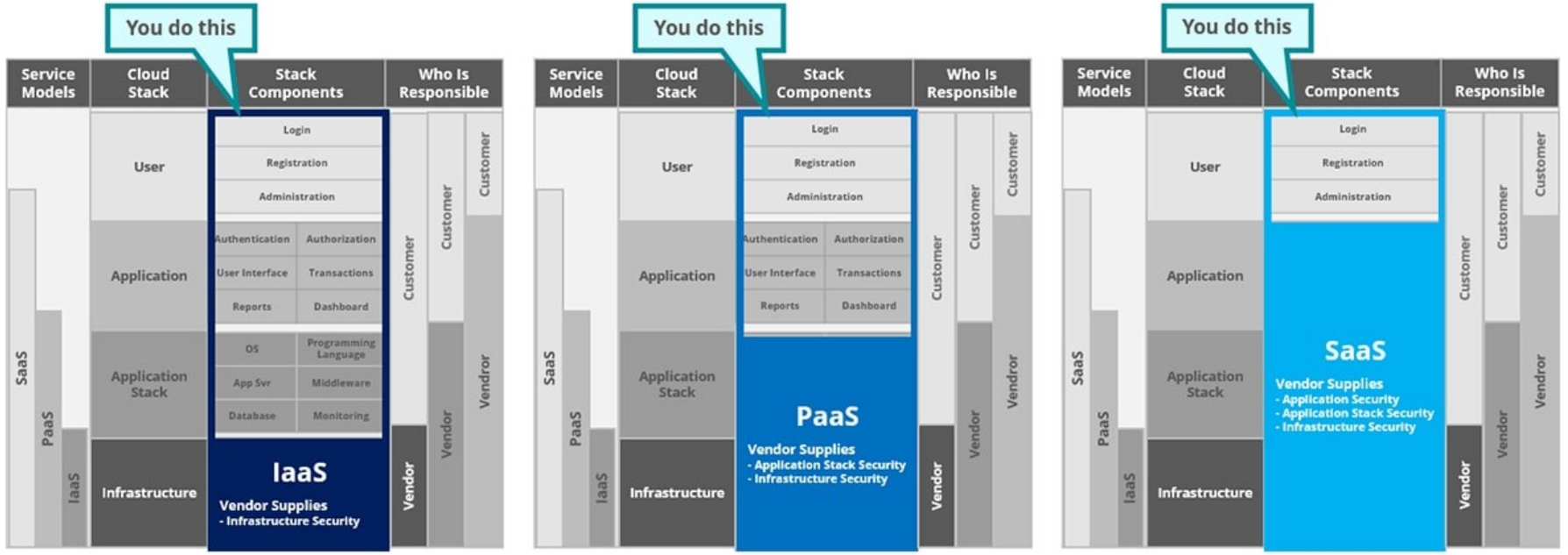
Guide to the shared responsibility model

■ USER'S RESPONSIBILITY ■ SERVICE PROVIDER'S RESPONSIBILITY

	EXAMPLES	APPLICATIONS	MIDDLEWARE	VIRTUALIZATION	DATA	O/S	NETWORKING	RUNTIME	SERVERS	STORAGE
SaaS	Dropbox, Salesforce CRM, Zoom, Microsoft 365, Google Workspace	■	■	■	■	■	■	■	■	■
PaaS	Microsoft Azure App Service, AWS Elastic Beanstalk, Google Kubernetes Engine, Red Hat OpenShift	■	■	■	■	■	■	■	■	■
IaaS	Microsoft Azure, Amazon Web Services (AWS), Google Compute Engine (GCE)	■	■	■	■	■	■	■	■	■

SOURCE: HTTPS://WWW.BMC.COM/BLOGS/SAAS-VS-PAAS-VS-IAAS-WHATS-THE-DIFFERENCE-AND-HOW-TO-CHOOSE/
ILLUSTRATION: IHUENG/GETTY IMAGES

https://www.techtarget.com/searchcloudcomputing/definition/shared-responsibility-model



https://www2.deloitte.com/us/en/pages/consulting/articles/clearing-the-air-around-cloud-shared-responsibility-models.html

A prezentáció anyagai használatának licencfeltétele: